UNCLASSIFIED

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

A CLASS OF MULTIPLE-ERROR-CORRECTING CODES AND THE DECODING SCHEME

IRVING S. REED

9 OCTOBER 1953

TECHNICAL REPORT NO. 44

UNCLASSIFIED

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

A CLASS OF MULTIPLE-ERROR-CORRECTING CODES AND THE DECODING SCHEME

Irving S. Reed

Technical Report No. 44

9 October 1953

ABSTRACT

A procedure for constructing one-error-correcting and two-error-detecting systematic codes has been introduced by R. W. Hamming. Some examples of n-error-correcting and (n+1) error-detecting systematic codes for the cases where both the code length and n+1 are powers of two are presented. The decoding scheme presented in this report differs from Hamming's scheme in that the encoded message will be extracted directly from the possibly corrupted received code by a majority testing of the redundant relations within the code. The general multinomial expansion formula for a Boolean function is discussed. A theorem about the relations satisfied by the highest or r-th degree coefficient of any vector or polynomial of a defined submodule of a particular Boolean ring is proved, and forms the basis for the general decoding principle.

CAMBRIDGE MASSACHUSETTS

A CLASS OF MULTIPLE-ERROR-CORRECTING CODES AND THE DECODING SCHEME

I. INTRODUCTION

A procedure for constructing one-error-correcting and two-error-detecting systematic codes was introduced in a recent study by R. W. Hamming.[1] It is the purpose of this report to exhibit some examples of n-error-correcting and (n + 1) error-detecting systematic codes for the cases where both the code length and (n + 1) are powers of two. The class of codes to be considered was developed by D. E. Muller in his recent work.[2]

The decoding scheme presented in this report differs from Hamming's scheme in that the encoded message will be extracted directly from the possibly corrupted received code by a majority testing of the redundant relations within the code. Hamming's scheme for n = 1 was dependent first on the location of a possible digit error in the code; secondly, on the correction of that digit; and lastly, on the extraction of the message from the corrected code. By circumventing Hamming's step of error location and correction, which is quite a severe problem when n is not equal to one, we have arrived at a decoding scheme that makes a natural use of the redundancy within the code as well as being conceptually simple and practical to implement.

In this report, some of the mathematical proofs of the methods discussed will be avoided for the sake of brevity of exposition. A more detailed mathematical analysis will appear elsewhere.

II. SOME MATHEMATICAL PRELIMINARIES

A code having n binary digits may be considered the element of a space, consisting of 2^n elements of the form

$$f = (f_0, \ldots f_{n-1})$$

where

$$(f_j = 0, 1) \text{ for } (j = 0, 1, 2, \ldots n - 1) \quad .$$

This space is technically an Abelian group if the sum of any two elements f and g in the space is defined as follows:

$$f \oplus g = (f_0, f_1, \ldots f_{n-1}) \oplus (g_0, g_1, \ldots g_{n-1}) = (f_0 \oplus g_0, f_1 \oplus g_1, \ldots f_{n-1} \oplus g_{n-1}) \quad ,$$

where $f_j \oplus g_j$ is the sum modulo two of the binary digits f_j and g_j for $(j = 0, 1, 2, \ldots n - 1)$. If multiplication by the binary scalar α is allowed as

$$\alpha f = \alpha(f_0, f_1, \ldots f_{n-1}) = (\alpha f_0, \alpha f_1, \ldots \alpha f_{n-1}) \quad ,$$

the Abelian group may be termed a generalized vector space of n-dimensions or a module. Finally, if the inner product operation

$$f \cdot g = (f_0, f_1, \ldots f_{n-1}) \cdot (g_0, g_1, \ldots g_{n-1}) = (f_0 g_0, f_1 g_1, \ldots f_{n-1} g_{n-1})$$

for f and g in the module is introduced, the space is a Boolean ring. The prime operation is defined to be

$$f' = f \oplus I$$

for f in the ring, and where I is the identity vector (1, 1, 1, ... 1).

Into this space one may further introduce a norm or length of a vector as follows:

$$\|f\| = \sum_{i=1}^{n} f_i$$

where Σ refers to ordinary addition. It is not difficult to see that the norm of the sum of two elements f and g in the ring or $\|f \oplus g\|$ is precisely the Hamming distance D(f, g) as defined in Ref. 1.

Now let n the dimension of the vector space be a power of two or $n = 2^m$. Let a vector of this space be of the form

$$f = (f_0, f_1, \ldots f_{2^m-1}) \quad ,$$

where f_j is a binary digit for $(j = 0, 1, \ldots 2^m-1)$. Now the vector f may be clearly expressed as

$$f = f_0 I_0 \oplus f_1 I_1 \oplus \ldots f_{2^m-1} I_{2^m-1} \quad , \tag{1}$$

where I_j is a unit vector with the digit one in j-th coordinate of the vector and zeros elsewhere for $(j = 0, 1, \ldots 2^m-1)$. Further, each unit vector I_j can be determined as a product of m vectors from the set of 2m vectors $x_1, x_2, x_3, \ldots x_m, x_1', x_2', x_3', \ldots x_m'$, where x_1 is a vector consisting of alternating zeros and ones, beginning with zero; x_2 is a vector consisting of alternating zero pairs and one pairs, beginning with a zero pair, and so forth, as follows:

$$\begin{aligned}
x_1 &= (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \ldots\ 0\ 1) \quad , \\
x_2 &= (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1 \ldots\ 1\ 1) \quad , \\
x_3 &= (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \ldots\ 1\ 1) \quad , \\
&\cdot \\
&\cdot \\
&\cdot \\
&\cdot \\
x_m &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \ldots\ 1\ 1) \quad .
\end{aligned} \tag{2}$$

If $x_k^{i_j}$ is defined to be x_k' for $i_k = 0$ and x_k for $i_k = 1$, then by the rules of Boolean algebra,

$$I_j = x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \quad , \tag{3}$$

where

$$j = \sum_{k=1}^{m} i_k 2^{k-1} \text{ with } (i_k = 0, 1) \text{ for } (j = 0, 1, \ldots m-1) \quad .$$

Combining Eqs. (1) and (3), we have

$$f = \sum_{j=0}^{2^m-1} f_j x_1^{i_1} x_2^{i_2} \ldots x_m^{i_m} \quad , \tag{4}$$

where $i_1, i_2, \ldots i_m$ are the digits of the binary representation of j, and where the summation

sign Σ is with respect to the sum operation $\oplus$. Equation (4) is the canonical expansion of any vector f in the Boolean algebra of 2^m dimensional vectors, consisting of binary digits.

If the identity $x_j' = I \oplus x_j$ and the distributive law of the algebra is used, Eq. (4) may be expanded to obtain the following polynomial in the x_j's:

$$f = g_0 \oplus g_1 x_1 \oplus \ldots \oplus g_m x_m \oplus g_{12} x_1 x_2 \oplus \ldots g_{m-1,\,m} x_{m-1} x_m \oplus \ldots$$
$$\ldots \oplus g_{12\ldots m} x_1 x_2 \ldots x_m \quad . \tag{5}$$

Equation (5) can be written more explicitly as

$$f = f(0,\ldots 0) \oplus \underset{1}{\Delta} f(0,\ldots 0)\, x_1 \oplus \ldots \oplus \underset{m}{\Delta} f(0,\ldots 0)\, x_m \oplus \overset{2}{\underset{12}{\Delta}} f(0,\ldots 0)\, x_1 x_2$$
$$\oplus \ldots \oplus \overset{m}{\underset{12\ldots m}{\Delta}} f(0,\ldots 0)\, x_1 x_2 \ldots x_m \quad , \tag{6}$$

where

$$f(i_1, \ldots i_m) = f_j \text{ when } j = \sum_{k=1}^{m} i_k 2^{k-1} \text{ for } i_k = 0, 1 \quad ,$$

and the Δ's are multiple partial differences, for example,

$$\underset{1}{\Delta} f(0) = f(1, 0, 0, \ldots) \oplus f(0, 0, 0, \ldots 0) \quad ,$$

$$\overset{2}{\underset{12}{\Delta}} f(0) = [f(1, 1, 0, \ldots) \oplus f(0, 1, 0, \ldots)] \oplus [f(1, 0, 0, \ldots) \oplus f(0, 0, 0, \ldots)] \quad ,$$

and so forth. The polynomial representation in Eq. (6) of the vector f supplies the relations between the coefficients of Eq. (5) and the scalars f_j of Eq. (4) for $(j = 0, 1, 2, \ldots 2^m - 1)$. This definition of the Δ's will be expanded in Sec. V.

III. THE GENERATION OF THE MULTIPLE ERROR ALLOWING CODES

Suppose that the dimension of the space considered in Sec. II is 2^m. Consider the set Φ_r^m of all polynomials of the form (5) of degree less than or equal to r where $r \leq m$. Each such polynomial must have the form

$$g_0 \oplus g_1 x_1 \oplus \ldots \oplus g_m x_m \oplus \ldots \oplus g_{12\ldots r} x_1 \cdots x_r \oplus \ldots \oplus g_{m-r,\,m-r+1,\ldots m}$$
$$x_{m-r} x_{m-r+1} \cdots x_m \quad , \tag{7}$$

and the sum of any two such polynomials is a member of the same set. This implies that Φ_r^m the set of all polynomials of type (7) or of degree less than or equal to r forms an Abelian group or submodule of the Boolean ring of 2^m dimensional vectors. Since Φ_r^m is a module, the Hamming distance between any two elements of Φ_r^m is the norm of a third element of Φ_r^m. This fact was exploited by D. E. Muller[2] in proving his Theorem 25. Muller's Theorem 25, in our terminology, may be expressed as follows:

Theorem A: – The norms of all non-zero vectors f of Φ_r^m satisfy

$$\|f\| \geq 2^{m-r} \text{ for } (m = 0, 1, 2, \ldots) \text{ and } r \leq m \quad .$$

We shall not prove this theorem in this section. It suffices to say that, with respect to our terminology, Muller proved the theorem by an induction on m, holding m – r constant, and the properties of the Hamming distance.

By the above theorem there is at least a distance 2^{m-r} between two elements of Φ_r^m and, as a consequence, there is an open Hamming sphere of radius 2^{m-r-1} about each element of Φ_r^m in Φ_r^m (the whole vector space) which does not intersect any other such sphere. This means that it is possible to associate each element of such a sphere with the element defining the sphere or what is the same to associate an element of Φ_r^m which is less than a distance 2^{m-r-1} from an element f of Φ_r^m with f.

In order to illustrate how a message may be coded into an error-detecting code of the type described above, consider the following example: Let m = 4 and r = 1, by (7) the vectors of Φ_1^4 are of the form

$$g_0 \oplus g_1 x_1 \oplus g_2 x_2 \oplus g_3 x_3 \oplus g_4 x_4 \quad . \tag{8}$$

Let the message consist of the five binary digits $(g_0, g_1, g_2, g_3, g_4)$. The code space Φ_1^4 may be regarded as generated by the four vector x_1, x_2, x_3, x_4 and the identity vector I which may be written explicitly as follows:

$$\begin{aligned}
x_1 &= (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \quad , \\
x_2 &= (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \quad , \\
x_3 &= (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \quad , \\
x_4 &= (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \quad , \\
I &= (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \quad .
\end{aligned} \tag{9}$$

The 32 vector codes of Φ_1^4 can be obtained by scalar multiplication of the vectors of (9) by the message digits g_0, g_1, g_2, g_3, g_4 in accordance with (8). For example, the message (0 1 1 0 0) has the code vector $g_1 x_1 \oplus g_2 x_2$ or

$$(0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0) \quad .$$

Each of the 32 codes will be a distance of at least eight from each other.

In order to practically generate the above code, one should note that the vector x_1 is the sequence of digits generated by the least significant binary stage B_1 of a binary counter of scale sixteen; x_2 is obtained from the second stage B_2; x_3 from the third stage B_3; and x_4 from the final stage B_4, as the counter goes through one period of its operation. If the message $(g_0, g_1, g_2, g_3, g_4)$ is stored in a binary register with stages A_0, A_1, A_2, A_3, A_4, then the switching function

$$C = A_0 \oplus A_1 B_1 \oplus A_2 B_2 \oplus A_3 B_3 \oplus A_4 B_4$$

will generate the code sequentially during one period of operation of the binary counter.

If one of the above codes of Φ_1^4 is corrupted during transmission so that no more than three errors are made, it is evidently possible by the previous discussion of this section to somehow extract the original message from the corrupted received code. The method by which this extraction may be accomplished will be shown by example in the next section and in general in the last section. It should be clear from the above example how the vectors of Φ_r^m may be generated for arbitrary r and m where $r \leq m$.

IV. DECODING CORRUPTED CODES OF Φ_r^m BY A MAJORITY TESTING OF REDUNDANCY RELATIONS

Let us first consider the coding space Φ_1^3. By (7), the vector of this space has the form

$$g_0 I \oplus g_1 x_1 \oplus g_2 x_2 \oplus g_3 x_3 \quad . \tag{10}$$

The message will consist of the four binary digits (g_0, g_1, g_2, g_3), and the generating vectors of the space are

$$\begin{aligned} x_1 &= (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \quad , \\ x_2 &= (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \quad , \\ x_3 &= (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \quad , \\ I &= (1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \quad . \end{aligned} \tag{11}$$

By (6) we have the following set of relations for the message digits g_j in terms of f_k, the code digits.

$$\begin{aligned} g_0 &= f(0, \ldots 0) = f_0 \quad , & \underset{12}{\Delta} f(0\ldots) &= f_0 \oplus f_1 \oplus f_2 \oplus f_3 = 0 \quad , \\ g_1 &= \underset{1}{\Delta} f(0\ldots) = f_0 \oplus f_1 \quad , & \underset{13}{\Delta} f(0\ldots) &= f_0 \oplus f_1 \oplus f_4 \oplus f_5 = 0 \quad , \\ g_2 &= \underset{2}{\Delta} f(0\ldots) = f_0 \oplus f_2 \quad , & \underset{23}{\Delta} f(0\ldots) &= f_0 \oplus f_2 \oplus f_4 \oplus f_6 = 0 \quad , \\ g_3 &= \underset{3}{\Delta} f(0\ldots) = f_0 \oplus f_4 \quad , & \underset{123}{\Delta} f(0\ldots) &= \sum_{i=0}^{7} f_i = 0 \quad . \end{aligned} \tag{12}$$

By (12) there are four relations which g_1 satisfies,

$$g_1 = f_0 \oplus f_1 = f_2 \oplus f_3 = f_4 \oplus f_5 = f_2 \oplus f_3 \oplus f_4 \oplus f_5 \oplus f_6 \oplus f_7 \quad .$$

By substituting the second and third relations into the fourth relation, we have

$$g_1 = g_1 \oplus g_1 \oplus f_6 \oplus f_7 = 0 \oplus f_6 \oplus f_7 = f_6 \oplus f_7 \quad .$$

Thus we obtain the four independent and disjoint relations for g_1,

$$g_1 = f_0 \oplus f_1 = f_2 \oplus f_3 = f_4 \oplus f_5 = f_6 \oplus f_7 \quad .$$

These four relations are disjoint in the sense that no two of the relations have variables in common. In a similar manner, we may obtain four independent and disjoint relations for both g_2 and g_3 so that g_1, g_2, g_3 may be expressed as

$$g_1 = f_0 \oplus f_1 = f_2 \oplus f_3 = f_4 \oplus f_5 = f_6 \oplus f_7 \quad ,$$

$$g_2 = f_0 \oplus f_2 = f_1 \oplus f_3 = f_4 \oplus f_6 = f_5 \oplus f_7 \quad ,$$

$$g_3 = f_0 \oplus f_4 = f_1 \oplus f_5 = f_2 \oplus f_6 = f_3 \oplus f_7 \quad .$$

Let us now suppose that the received code is the vector $(f_0, f_1, \ldots f_7)$. If there were no error in transmission of the code, all of the above relations would hold. If there were one error, three out of four of the relations would hold. If there were two errors, at least two of the g_j's would have two out of four incorrect relations. Then g_1, g_2, g_3 may be determined uniquely if one or no error occurred during transmission, and two errors may always be detected by making a majority decision test on the arithmetic sum of the values of the four relations for each g_j $(j = 1, 2, 3)$. In order to state this criterion more explicitly, let the values of the four relations for g_j be denoted by $r_{j1}, r_{j2}, r_{j3}, r_{j4}$ for $(j = 1, 2, 3)$, and let S_j be the arithmetic sum of $r_{j1}, r_{j2}, r_{j3}, r_{j4}$ or

$$S_j = \sum_{i=1}^{4} r_{ji} \quad .$$

Then the majority decision test for g_j is

$$\begin{aligned} g_j &= 0 && \text{if } 0 \leq S_j < 2 \quad , \\ g_j &\text{ is indeterminate} && \text{if } S_j = 2 \quad , \\ g_j &= 1 && \text{if } 2 < S_j \leq 4 \text{ for } (j = 1, 2, 3) \quad . \end{aligned} \tag{13}$$

With the assumption that the received code is no more than two digits in error, the majority test (13) will determine g_1, g_2, g_3 uniquely for only one or no errors, and reject the code as meaningless in the case of two errors. In the case of one error or less, g_1, g_2, g_3 may be assumed now to be determined; it remains to determine g_0. In order to find g_0, note that if, as g_1, g_2, g_3 are found, the vectors g_1x_1, g_2x_2, g_3x_3 are added successively to the received vector, by (10) we will end with either the vector g_0I in the case of no error or with a vector of distance one from g_0I. Thus to detect g_0 the following majority decision test will suffice:

$$\begin{aligned} g_0 &= 0 \text{ if } \sum_{i=0}^{7} m_i < 4 \quad , \\ &= 1 \text{ if } \sum_{i=0}^{7} m_i > 4 \quad , \end{aligned} \tag{14}$$

where m_i are the digits of the code after extraction of digits g_1, g_2, g_3 in accordance with the above procedure.

The above method of decoding may be illustrated by the following example: Suppose that the message sent was (1 0 1 1), and that during transmission an error was made in the fifth

digit of the original code (1 1 0 0 0 0 1 1) so that the received code had the form (1 1 0 0 1 0 1 1). We first test for g_1, g_2, g_3 by (12) and find $g_1 = 0$, $g_2 = 1$ and $g_3 = 1$. Using (11), we add $g_1x_1 \oplus g_2x_2 \oplus g_3x_3$ to the code, obtaining

$$0(0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \oplus (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \oplus (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \oplus (1\ 1\ 0\ 0\ 1\ 0\ 1\ 1)$$
$$= (1\ 1\ 1\ 1\ 0\ 1\ 1\ 1) = (m_0, m_1, m_2, \ldots m_3) \quad .$$

Finally, by (14)

$$g_0 = 1 \quad , \quad \text{since} \sum_{i=0}^{7} m_i = 7 > 1 \quad .$$

Although Φ_1^3 is none other than an example of a set of one-error-correcting and two-error-detecting codes of the type described by Hamming in Ref. 1, the method of decoding considered above is different. Our procedure of decoding is advantageous in that it may be generalized in a natural way to include any of the coding spaces Φ_r^m of Sec. II. Before we consider this generalization by further examples, let us note a tabular way of representing the redundancy relations (12).

If the digits or variables of each relation are connected by lines for each of the vectors x_1, x_2, x_3 as

$$x_1 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \quad ,$$

$$x_2 = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \quad ,$$

$$x_3 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \quad , \qquad (15)$$

the relations of (12) become almost self-evident by their simplicity with respect to order and symmetry. This simplicity makes it possible to discover redundancy relations for more general spaces Φ_r^m without resorting to an algebraic approach similar to the one used to obtain (12).

As a second example of our decoding procedure, consider the coding space Φ_1^4 introduced in the latter part of Sec. III. Each vector of this space has the form of (8), where the generating vectors are x_1, x_2, x_3, x_4 and I of (9). The first-degree redundancy relations may be determined in a manner similar to the above example and represented in a tabular manner similar to (15) as follows:

$$x_1 = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1) \quad ,$$

$$x_2 = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1) \quad ,$$

$$x_3 = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1) \quad ,$$

$$x_4 = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1) \quad . \qquad (16)$$

For instance, the eight independent and joint relations for g_1 are

$$g_1 = f_{2i} \oplus f_{2i+1} \quad \text{for} \quad (i = 0, 1, \ldots 7) \quad .$$

If the eight values of the redundancy relations for g_j are labeled $r_{j1}, r_{j2}, \ldots r_{j8}$ for $(j = 1, 2, 3, 4)$, and S_j is defined by

$$S_j = \sum_{i=1}^{8} r_{ji} \quad ,$$

then, by an argument similar to that used in the previous example, the majority decision test for g_j is as follows:

$$g_j = 0 \qquad \text{if} \quad 0 \leqslant S_j < 4 \quad ,$$

$$g_j \text{ is indeterminate} \qquad \text{if} \quad S_j = 2 \quad ,$$

$$g_j = 1 \qquad \text{if} \quad 4 \leqslant S_j \leqslant 8 \quad \text{for} \quad (j = 1, 2, 3, 4) \quad . \tag{17}$$

In order to determine g_0, we first add the determined vectors $g_j x_j$ to the received message, assuming, of course, that no g_j is indeterminate, and we are left with the zero-degree polynomial ϕ_0^4, possibly corrupted by errors. If there had been no errors, there would be sixteen zero-degree relations which g_0 satisfies, or

$$g_0 = m_j \quad \text{for} \quad (j = 0, 1, 2, \ldots 15) \quad ,$$

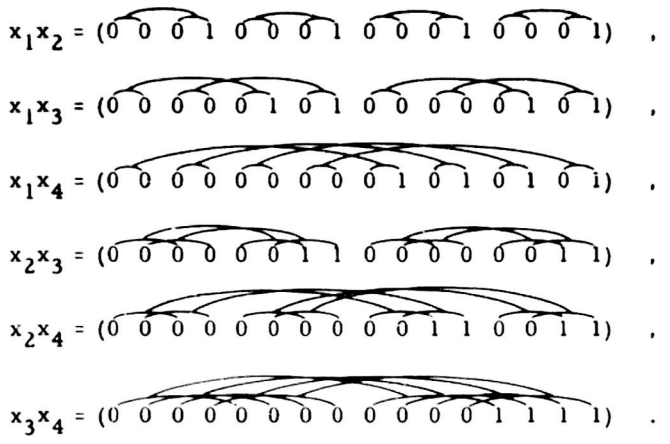
where, as in (14), m_j are the digits of the code after extraction of g_1, g_2, g_3 and g_4. Thus g_0 is determined by the majority decision test

$$g_0 = 0 \quad \text{if} \quad \sum_{i=0}^{15} m_i < 8 \quad ,$$

$$= 1 \quad \text{if} \quad \sum_{i=0}^{15} m_i > 8 \quad . \tag{18}$$

For the above example, three errors may be made in code and the correct message obtains. If four errors are made, some of the message digits are indeterminate. It is of some interest to note that, for some cases of five errors in the code, the message may be extracted correctly. For example, suppose that the message was (0 0 0 0 0) and that the received code was (1 1 0 0 1 0 1 0 1 0 0 0 0 0 0 0). Clearly, the correct message will be extracted from this code by the above procedure.

As a final example of coding and decoding scheme, consider ϕ_2^4. This space is generated by x_1, x_2, x_3, x_4 of (16) and I, as well as the quadratic variables $x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4$. The latter six vectors may be presented in the following tabular manner:



The messages for this example will be 11 binary digit numbers of the form $(g_0, g_1, g_2, g_3, g_4, g_{12}, g_{13}, g_{14}, g_{23}, g_{24}, g_{34})$. Each code will be sent as a vector of the form

$$g_0 \oplus g_1x_1 \oplus g_2x_2 \oplus g_3x_3 \oplus g_4x_4 \oplus g_{12}x_1x_2 \oplus g_{13}x_1x_3 \oplus g_{14}x_1x_4 \oplus g_{23}x_2x_3 \oplus g_{24}x_2x_4 \oplus g_{34}x_3x_4 \quad .$$

The second-degree coefficients g_{ij} of the received message are extracted first with a majority decision based on the redundancy relations illustrated in (19). Next, assuming that no indeterminacy occurred in the second-degree coefficients, the vectors $g_{ij}x_ix_j$ are added to the received code, after which we are left with a residual code from which the first-degree coefficients g_1, g_2, g_3, g_4 may be extracted by test (17). Finally, the zero-degree coefficient g_0 may be determined by test (18) after adding the vector $g_1x_1, g_2x_2, g_3x_3, g_4x_4$ to the residual code.

This example illustrates the general principle of decoding the particular class of codes under consideration. The highest degree coefficients of a received code are extracted first; then these terms of the polynomial are subtracted out of the code, thereby leaving a residual code of the next lower degree than the original code in the special case of no errors. The operation is repeated over and over on the successive residual codes until either an indeterminacy occurs or until g_0 is extracted.

The relations of (19) illustrate the fact that there are four redundancy relations each of four variables for the second-degree coefficients g_{ij}. For example, the redundancy relations for g_{12} are

$$g_{12} = f_{4i} \oplus f_{4i+1} \oplus f_{4i+2} \oplus f_{4i+3} \quad \text{for} \quad (i = 0, 1, 2, 3) \quad . \tag{20}$$

In general, these relations will allow only one error; two errors will lead to indeterminacy. This is another example of Hamming's one-error-correction and two-error-detection codes.

It should be noted that the majority decision tests used in the above examples were, in general, overdeterminate. For instance, in the first example, if one error had been made,

no more than one error would remain in the residual code after determining g_1, g_2, g_3. On the other hand, if two errors had occurred, the process of extraction would have ended before g_0 could be determined. Thus a test of only the following type would be necessary:

$$g_0 = 0 \text{ if } m_{i1} + m_{i2} + m_{i3} \leq 1 \quad ,$$

$$g_1 = 1 \text{ if } m_{i1} + m_{i2} + m_{i3} \geq 2 \quad ,$$

where i_1, i_2, i_3 are any three distinct numbers between zero and seven, inclusive. Refinements such as this, however, do not destroy the validity of the previous tests.

V. THE GENERAL DECODING PRINCIPLE

To study the general decoding scheme, illustrated by example in Sec. IV, it will be necessary to consider the general multinomial expansion formula (6) more carefully. Let us first define the multiple differences, used in (6), in more detail.

As in (6), $f(i_1, \ldots i_m)$ is defined as

$$f(i_1, \ldots i_m) = f_j \text{ when } j = \sum_{k=1}^{m} i_k 2^{k-1} \text{ for } (i_k = 0, 1) \quad . \tag{21}$$

The general multiple partial difference

$$\overset{p}{\underset{k_1, k_2, \ldots k_p}{\Delta}} f(i_1, i_2, \ldots i_m)$$

is defined inductively as

$$\overset{}{\underset{k}{\Delta}} f(i_1, \ldots i_m) = f(i_1, \ldots i_{k-1}, i_k \oplus 1, i_{k+1}, \ldots i_m) \oplus f(i_1, \ldots i_k, \ldots i_m)$$

$$\overset{p}{\underset{k_1 k_2, \ldots k_p}{\Delta}} f(i_1, \ldots i_m) = \overset{p-1}{\underset{k_1, \ldots k_{p-1}}{\Delta}} f(i_1, \ldots i_{k_{p-1}}, i_{k_p} \oplus 1, i_{k_{p+1}}, \ldots i_m)$$

$$+ \overset{p-1}{\underset{k_1, \ldots k_{p-1}}{\Delta}} f(i_1, \ldots i_m) \quad . \tag{22}$$

With these definitions it is possible to prove by induction the validity and uniqueness of expansion (6) for any Boolean algebra of m variables and, in particular, for the Boolean algebra of 2^m dimensional vectors as described in Sec. II.

One evident consequence of (21) is the identity

$$f(i_1, \ldots i_{k-1} i_k \oplus 1, i_{k+1}, \ldots i_m) = f_{i+(-1)^{i_k} 2^{k-1}} \quad . \tag{23}$$

By the use of (23) it is possible to write (22) explicitly in terms of the f_i as

$$\Delta_{k} f(i_1, \ldots i_m) = f_i \oplus f_{i+(-1)^{i_k} 2^{k-1}}$$

and

$$\Delta_{k_1, k_2, \ldots k_p} f(i_1, \ldots i_m) = \sum_{i=1}^{2^{p-1}} f_{j_i} \oplus \sum_{i=1}^{2^{p-1}} f_{j_{i+(-1)^{i_{k_p}} 2^{k_p - 1}}}$$

where

$$\Delta_{k_1, k_2, \ldots k_{p-1}} f(i_1, \ldots i_m) = \sum_{i=1}^{2^{p-1}} f_{j_i} \quad \text{and} \quad j_i \neq j_s + (-1)^{i_{k_p}} 2^{k_p - 1}$$

$$\text{for } (i, s = 1, \ldots 2^{p-1}) \quad . \tag{24}$$

We are now in a position to prove the following fundamental theorem on which the general decoding principle of the class of codes under consideration rests.

Theorem B: – Each highest or r-th degree coefficient of any vector or polynomial f of Φ_r^m satisfies exactly 2^{m-r} disjoint relations where each relation has precisely the form

$$\sum_{k=1}^{2^r} f_{i_k} \quad ,$$

where i_k are distinct numbers from the set $(0, 1, 2, \ldots 2^m - 1)$ for $(k = 1, 2, \ldots 2^r)$. Disjointness of relations means that no two relations have variables f_i in common.

Proof: – Choose m and r. By (6), (7) and (24), the highest degree coefficients for an f of Φ_r^m are

$$g_{k_1 \ldots k_r} = \Delta_{k_1 k_2 \ldots k_r}^{r} f(0, \ldots 0) = \sum_{i=1}^{2^r} f_{j_i} \quad , \tag{25}$$

where k_j are distinct integers from the set $(1, 2, \ldots m)$ for $(j = 1, \ldots r)$, and j_i are distinct integers from the set $(0, 1, \ldots 2^m - 1)$ for $(i = 1, 2, \ldots 2^r)$. Moreover,

$$\Delta_{k_1 \ldots k_r n_1 n_2 \ldots n_t} f(0, \ldots 0) = 0 \tag{26}$$

for $t \geq 1$, and k_j and n_i are distinct integers from the set $(1, 2, \ldots m)$ for $(j = 1, \ldots t)$.

Let $k_1, k_2 \ldots k_r$ be a distinct set of integers from the set $(1, 2, \ldots m)$. Then, by (26) and (22),

$$\Delta_{k_1 \ldots k_r n_1}^{r+1} f(0, \ldots 0) = \Delta_{k_1 \ldots k_r}^{r} f(0, \ldots 0) \oplus \Delta_{k_1 \ldots k_r}^{r} f(0, \ldots 1, \ldots 0) = 0 \quad , \tag{27}$$

where n_1 is any one of the $m - r$ integers from the set $(1, 2, \ldots m)$ which is distinct from the integers $(k_1, k_2, \ldots k_r)$. Thus, by (24) and (25), we have exhibited $m - r$ new relations of the

form required by the theorem. Each of these new relations is distinguished by the fact that the digit one appears only in the n_1-th position of the function $f(i_1, \ldots i_m)$ operated on by

$$\overset{r}{\underset{k_1 \ldots k_r}{\Delta}} \quad .$$

Now define $f[n_1, n_2, \ldots n_t]$ to be $f(i_1, i_2, \ldots i_m)$ with $i_k = 1$ for $k = n_1, n_2, \ldots n_t$ and $i_k = 0$ otherwise. The theorem will be proved by induction on the subscript of n. Assume therefore that

$$\overset{r+s-1}{\underset{k_1 k_2 \ldots k_r n_1 n_2 \ldots n_{s-1}}{\Delta}} f(0, 0, \ldots 0) = \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f(0, 0, \ldots 0) \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_1, n_2 \ldots n_{s-1}] \quad . \tag{28}$$

Now, by (22) and (26) and the induction hypothesis (28),

$$\begin{aligned}
\overset{r+s}{\underset{k_1 \ldots k_r n_1 \ldots n_s}{\Delta}} f(0, 0, \ldots 0) &= \overset{}{\underset{n_s}{\Delta}} \left(\overset{r+s-1}{\underset{k_1 \ldots k_r n_1 \ldots n_{s-1}}{\Delta}} f(0, 0, \ldots 0) \right) , \\
&= \overset{}{\underset{n_s}{\Delta}} \left(\overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f(0, \ldots 0) \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_1, \ldots n_{s-1}] \right) , \\
&= \overset{r}{\underset{k_1, \ldots k_r}{\Delta}} f(0, 0, \ldots 0) \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_1, \ldots n_{s-1}] , \\
&\quad \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_s] \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_1, \ldots n_s] = 0 \quad .
\end{aligned}$$

Now, by (27) and (28), the two middle terms are equal to

$$\overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f(0, 0, \ldots 0) \quad ,$$

and therefore their sum modulo 2 is zero. Hence

$$\overset{r+s}{\underset{k_1 \ldots n_s}{\Delta}} f(0, \ldots 0) = \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f(0, \ldots 0) \oplus \overset{r}{\underset{k_1 \ldots k_r}{\Delta}} f[n_1, \ldots n_s] = 0 \quad ,$$

and the induction is complete. The theorem is proved when we observe that the relation

$$\Delta^{r+s}_{k_1 \ldots n_s} f(0, \ldots 0) = 0 \text{ contributes } \binom{m-r}{s} \text{ distinct relations}$$

$$\Delta_{k_1 \ldots k_r} f(0, \ldots 0) = \Delta_{k_1 \ldots k_r} f[n_1, n_2 \ldots n_s] \quad ,$$

since there are $\binom{m-r}{s}$ ways of choosing s integers from m − r integers. Using all the relations (26) for the particular set $k_1 \ldots k_r$ and t = 1 to t = m − r and the relation (25), we get

$$1 + \sum_{t=1}^{m-r} \binom{m-r}{t} = 2^{m-r}$$

distinct relations for $g_{k_1, k_2, \ldots k_r}$. Since these relations exhaust all variables f_{i_k}, the theorem is proved.

The above theorem shows that the generalization of the decoding principle, discussed in the last section, obtains. The majority decision test for the general case can clearly be used to extract the r-th degree coefficients of I_r^m, where the relations used for the test are the 2^{m-r} relations of Theorem B. The (r − 1)-th degree coefficients are then extracted the same way after the determined r-th order terms have been subtracted or added into the received code. This process is continued for the r − 2, r − 3, ... degree coefficients until the message is extracted or an indeterminacy is reached.

VI. CONCLUSIONS

There are two or three generalizations of the codes and the methods of decoding. In Ref. 2, Muller discusses a possible set of codes other than binary length of 2^m. Another generalization obtains where the polynomials are considered over a field other than characteristic two; i.e., ternary codes, etc. Lastly, it appears from some work of T. A. Kalin that an error-correction scheme of the type considered by Hamming may generalize to the coding space Φ_r^m in a rather natural way.

ACKNOWLEDGMENTS

The author expresses his appreciation to E. B. Rawson for nis assistance in the construction of the second example of Section 4; to G. P. Dinneen for his help in the simplification of Theorem B; and to T. A. Kalin, W.B. Davenport, Jr., D. E. Muller and O. G. Selfridge for several useful discussions.

REFERENCES

1. R. W. Hamming, Bell System Tech. J. 26, No. 2, 147 (April 1950).
2. D. E. Muller, "Metric Properties of Boolean Algebra and Their Application to Switching Circuits," Report No. 46, Digital Computer Laboratory, University of Illinois (April 1953).